

DE10020561

Patent number: DE10020561
Publication date: 2001-04-12
Inventor: LANG JUERGEN (DE); MEYER BERND (DE)
Applicant: DEUTSCHE POST AG (DE)
Classification:
- international: **H04L9/32; H04L9/32; (IPC1-7): H04L9/32; G06F13/00**
- european: **H04L9/32**
Application number: DE20001020561 20000427
Priority number(s): DE20001020561 20000427; DE19991048319 19991007

Also published as:

-  W O0125879 (A3)
-  W O0125879 (A2)
-  E P1222512 (A3)
-  E P1222512 (A2)
-  CA 2425176 (A1)

[more >>](#)[Report a data error here](#)**Abstract of DE10020561**

The invention relates to a security module characterized in that said module contains a data input port via which information can be inputted into the security modul. The security module has at least two data output ports whereby data can be outputted via a first data output port and transferred to an authentication unit and whereby data can be outputted via a second data output port. Said data can be transferred to a document to be exported. Said security module has at least two combination machines. A first combination machine generates a first result value for a first data output and a second combination machine generates a result value for the second data output. The invention relates to the use of a security module for generating forge-proof documents.

Data supplied from the **esp@cenet** database - Worldwide

⑯ BUNDESREPUBLIK

DEUTSCHLAND



DEUTSCHES

PATENT- UND

MARKENAMT

Offenlegungsschrift

⑯ DE 100 20 561 A 1

⑯ Int. Cl. 7:
H 04 L 9/32
G 06 F 13/00

DE 100 20 561 A 1

⑯ Aktenzeichen: 100 20 561.5
⑯ Anmeldetag: 27. 4. 2000
⑯ Offenlegungstag: 12. 4. 2001

⑯ Innere Priorität:

199 48 319. 1 07. 10. 1999

⑯ Anmelder:

Deutsche Post AG, 53175 Bonn, DE

⑯ Vertreter:

Jostarndt Thul Patentanwälte, 52076 Aachen

⑯ Erfinder:

Lang, Jürgen, Dr., 51429 Bergisch Gladbach, DE;
Meyer, Bernd, 53639 Königswinter, DE

⑯ Entgegenhaltungen:

DE	44 42 357 A1
EP	8 86 409 A2
EP	7 22 151 A2

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

⑯ Sicherungsmodul und Verfahren zur Erstellung fälschungssicherer Dokumente

⑯ Erfindungsgemäß zeichnet sich das Sicherungsmodul dadurch aus, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang Daten ausgegeben werden können, die an eine Bescheinigungsstelle übertragen werden und wobei durch einen zweiten Datenausgang Daten ausgegeben werden, die auf ein auszugebendes Dokument übertragen werden können, mit wenigstens zwei Kombinationsmaschinen, wobei eine erste der Kombinationsmaschinen einen Ergebniswert für den ersten Datenausgang erzeugt und wobei eine zweite Kombinationsmaschine einen Ergebniswert für den zweiten Datenausgang erzeugt. Die Erfindung betrifft ferner den Einsatz des Sicherungsmoduls zur Erstellung fälschungssicherer Dokumente.

DE 100 20 561 A 1

Beschreibung

Die Erfindung betrifft ein Sicherungsmodul.

Die Erfindung betrifft ferner ein Verfahren zur Erstellung fälschungssicherer Dokumente, wobei Eingangsdaten in einen Dateneingang eines Sicherungsmoduls eingegeben werden.

Der Erfindung liegt die Aufgabe zugrunde, ein Sicherungsmodul zu schaffen, mit dem fälschungssichere Dokumente erzeugt werden können.

Erfindungsgemäß wird diese Aufgabe dadurch gelöst, dass ein Sicherungsmodul so gestaltet wird, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang Daten ausgegeben werden können, die an eine Bescheinigungsstelle übertragen werden und wobei durch einen zweiten Datenausgang Daten ausgegeben werden, die auf ein auszugebendes Dokument übertragen werden können, dass das Sicherungsmodul wenigstens zwei Kombinationsmaschinen enthält, wobei eine erste der Kombinationsmaschinen einen Ergebniswert für den ersten Datenausgang erzeugt und wobei eine zweite Kombinationsmaschine einen Ergebniswert für den zweiten Datenausgang erzeugt.

Zur Erhöhung der Datensicherheit ist es zweckmäßig, dass das Sicherungsmodul so gestaltet wird, dass es einen Geheimnisgenerator enthält, der ein nicht vorhersehbares Geheimnis erzeugt.

Hierbei ist es besonders vorteilhaft, dass der Geheimnisgenerator mit der ersten Kombinationsmaschine und/oder der zweiten Kombinationsmaschine so verbunden ist, dass ein von dem Geheimnisgenerator erzeugtes Geheimnis in die erste Kombinationsmaschine und/oder die zweite Kombinationsmaschine eingeht.

Für eine Anwendung des Sicherungsmoduls in Systemen, in denen eine Abrechnung, insbesondere eine Abrechnung von Leistungen, erfolgt, ist es besonders zweckmäßig, dass das Sicherungsmodul so gestaltet ist, dass es ein Identifikationsregister enthält, wobei ein Ausgangswert des Identifikationsregisters so mit der ersten Kombinationsmaschine verbunden ist, dass in eine von der ersten Kombinationsmaschine ausgegebene Datenkombination ein Wert des Identifikationsregisters eingeht.

Eine weitere Erhöhung der Datensicherheit lässt sich vor teilhafterweise dadurch erzielen, dass das Sicherungsmodul wenigstens eine Verschlüsselungsmaschine enthält, welche einen Ausgangswert einer der Kombinationsmaschinen verschlüsselt.

Hierbei ist es zweckmäßig, dass die Verschlüsselungsmaschine mit einem Schlüsselregister verbunden ist, wobei wenigstens ein in dem Schlüsselregister enthalter Wert in der Verschlüsselungsmaschine zur Verschlüsselung eingesetzt werden kann.

Eine zweckmäßige Implementation des Sicherungsmoduls zeichnet sich dadurch aus, dass es eine Hash-Maschine enthält.

Weitere Vorteile, Besonderheiten und zweckmäßige Weiterbildungen der Erfindung ergeben sich aus den Unteran sprüchen und der nachfolgenden Darstellung bevorzugter Ausführungsbeispiele anhand der Zeichnung.

Die Zeichnung, Fig. 1, zeigt eine Prinzipdarstellung eines für die Erstellung fälschungssicherer Dokumente geeigneten Sicherungsmoduls.

Das in Fig. 1 dargestellte Sicherungsmodul weist einen Dateneingang auf, durch den Informationen in das Sicherungsmodul eingegeben werden können.

Das Sicherungsmodul weist ferner zwei Datenausgänge

DA1 und DA2 auf.

Durch den ersten Datenausgang DA1 können Daten ausgegeben werden, die an eine externe Stelle, beispielsweise eine Bescheinigungsstelle, übertragen werden.

5 Durch den zweiten Datenausgang DA2 können Daten auf ein auszugebendes Dokument übertragen werden.

Das Sicherungsmodul weist ferner wenigstens zwei Kombinationsmaschinen K1, K2 auf. Die erste Kombinationsmaschine K1 erzeugt einen Ergebniswert für den ersten Datenausgang DA1. Die zweite Kombinationsmaschine K2 erzeugt einen Ergebniswert für den zweiten Datenausgang DA2.

15 Ferner enthält das Sicherungsmodul wenigstens einen Geheimnisgenerator GG, der ein nicht vorhersehbares Geheimnis erzeugt. Der Geheimnisgenerator ist sowohl mit der ersten Kombinationsmaschine K1 als auch mit der zweiten Kombinationsmaschine K2 verbunden. Die Verbindung zwischen dem Geheimnisgenerator GG und der Kombinationsmaschine K2 erfolgt vorzugsweise über einen Zwischen speicher.

20 Der Zwischenspeicher hat vorzugsweise die Funktion, das im Geheimnisgenerator erzeugte Geheimnis temporär zu speichern.

25 Das Sicherungsmodul enthält ferner ein Identifikationsregister, das so mit der ersten Kombinationsmaschine K1 verbunden ist, dass in eine von der ersten Kombinationsmaschine ausgegebene Datenkombination ein Wert des Identifikationsregisters eingeht.

30 Eine in dem Sicherungsmodul enthaltene Verschlüsselungsmaschine ist so programmiert, dass sie einen Ausgangswert einer der Kombinationsmaschinen verschlüsselt, im dargestellten Fall der Kombinationsmaschine K1.

35 Um Speicherplatz zu sparen, ist es zweckmäßig, ein asymmetrisches Schlüsselpaar nach einem geeigneten Sicherheitsstandard wie beispielsweise RSA zur Verschlüsselung und Signatur einzusetzen. Da keine beliebigen, vom Benutzer vorgegebenen Texte in die Verschlüsselung, Signatur und Hashwertbildung einfließen können, ist dieser Schritt zu rechtfertigen.

40 Die Schlüssellänge beträgt vorzugsweise wenigstens 128 bit, zweckmäßigerweise deutlich mehr, beispielsweise mindestens 1024 bit, RSA.

45 Die Erzeugung des Hash-Wertes erfolgt vorzugsweise nach dem Standard SHA-1. Die Hash-Maschine verknüpft eingebrachte Daten irreversibel mit einem Geheimnis. Hier durch entsteht bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis, ohne dass Rückschlüsse auf das Geheimnis möglich sind. Vorzugsweise ist das Geheimnis temporär, da hierdurch die Sicherheit gesteigert wird. Dies ist jedoch nicht notwendig. Beispielsweise kann das Geheimnis fest in einem Datenspeicher eingegeben sein.

50 Nachfolgend wird die Funktionsweise des Sicherungsmoduls an dem besonders bevorzugten Beispiel der Freimachung von Briefsendungen erläutert.

55 Das Sicherungsmodul eignet sich jedoch gleichermaßen für andere Verschlüsselungszwecke. Eine Verwendung des Sicherungsmoduls zur Erzeugung fälschungssicherer Dokumente ist besonders zweckmäßig. Der Begriff fälschungssichere Dokumente ist in keiner Weise einschränkend zu verstehen. Neben den beispielhaft dargestellten Freimachungs vermerken kann es sich bei dem fälschungssicheren Dokumenten auch um Fahrkarten oder Eintrittskarten handeln. Durch die Möglichkeit, jede einzelne Dokumentenerzeugung auf der Grundlage von individuellen Daten durchzuführen, können auch einmalige Dokumente wie persönliche Ausweise, Platzkarten oder Listen mit personifizierten Werten erzeugt werden.

Das Sicherungsmodul bearbeitet vorzugsweise individuallisierbare Informationen, beispielsweise Zertifikate und digitale signierte Lizenzen.

Bei einem bevorzugten Beispiel eines Einsatzes für die Freimachung von Briefen im Bereich der Deutschen Post AG geschieht dies wie folgt:

Eine digitale Signatur ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt (vgl. SigG §2, Abs. 1). Unter Benutzung der hier verwandten Terminologie ist eine Prüfstelle in der Lage, die digitale Signatur eines Dokumentherstellers und somit sowohl dessen Identität als auch die Unverfälschtheit der im Dokument enthaltenen Daten zu prüfen, wenn ihr der öffentliche Signaturschlüssel des Dokumentherstellers, der mit einem Signaturschlüssel-Zertifikat versehen ist, zur Verfügung steht.

Jedes hergestellte Sicherungsmodul wird von dem Kundensystemhersteller "digital lizenziert". Die Bescheinigungsstelle erstellt zur Kommunikation mit den Sicherungsmodulen eine eigene signierte Kommunikationslizenz im gleichen Format.

Die Zertifizierung und signierte Lizenzierung erfolgen vorzugsweise wie folgt:

Das Sicherungsmodul erzeugt intern ein Schlüsselpaar, dessen öffentlicher Schlüssel P_{SB} (Public Key) unter Benutzung des privaten Signaturschlüssels des Kundensystemanbieters S_I (Issuer) digital lizenziert wird. Der öffentliche Schlüssel des Kundensystemanbieters P_I ist ebenso wie der öffentliche Schlüssel der Bescheinigungsstelle von der Zertifizierungsstelle (CA) erstellt und zertifiziert und steht dort zur Prüfung zur Verfügung.

Insgesamt werden im System folgende Schlüssel, Zertifikate und signierte Lizenzen verwendet.

In dem Sicherungsmodul stehen ein privater Schlüssel des Sicherungsmoduls, ein öffentlicher Schlüssel des Sicherungsmoduls und eine durch den Kundensystemanbieter (Issuer) signierte Lizenz des öffentlichen Schlüssels des Sicherungsmoduls.

In der Bescheinigungsstelle stehen vorzugsweise mindestens ein privater Schlüssel der Bescheinigungsstelle und ein öffentlicher Schlüssel der Bescheinigungsstelle zur Verfügung.

Das Sicherungsmodul prüft die Gültigkeit der signierten Lizenz, beispielsweise durch Kontaktierung einer Zertifizierungsstelle.

Die Bescheinigungsstelle prüft die Gültigkeit der signierten Lizenz eines Sicherungsmoduls – und somit die Identität des Kundensystemanbieters (Issuer) über die Identität der per Attributeneintrag im Zertifikat für den Kundensystemanbieter verantwortlichen natürlichen Person – durch Kontaktierung der Zertifizierungsstelle.

Der Herausgeber der Signaturkarten stellt sicher, dass entsprechende Attribute (z. B. Prokura zur Ausgabe von Lizenzen für Sicherungsmodule) ausschließlich in Abstimmung mit der Stelle, bei der die fälschungssicheren Dokumente eingereicht werden, vergeben werden.

Ein regulärer Austausch des Schlüsselpaars des Sicherungsmoduls ist nicht notwendig, jedoch möglich. Die vorgesehene Gültigkeitsdauer der Schlüssel ist möglichst lang, um die Benutzerfreundlichkeit zu erhöhen. Die Gültigkeitsdauer der Schlüssel des Sicherungsmoduls beträgt vorzugsweise mehrere Monate bis Jahre, wobei Werte zwischen drei Monaten und 15 Jahren infrage kommen. Vorzugsweise beträgt die Gültigkeitsdauer zwischen 3 Jahren und 10 Jahren, wobei sich etwa 6 Jahre besonders eignen.

Der Kundensystemhersteller ist berechtigt, die Schlüssel, mit denen er die Lizenzen der ausgegebenen Sicherungsmodulen digital lizenziert, jederzeit zu wechseln. Der Kundensystemhersteller ist verpflichtet, die Signaturschlüssel, mit denen er die Lizenzen der ausgegebenen Sicherungsmodulen digital signiert, nach spätestens einem Jahr zu wechseln und hierbei den alten Signaturschlüssel sperren zu lassen. Der Kundensystemhersteller kennzeichnet die Signaturschlüssel in Abstimmung mit der Bescheinigungsstelle.

Eine zur Prüfung der fälschungssicheren Dokumente berechtigte Stelle lehnt Transaktionen bei Feststellung einer Korrumperung eines Schlüssels ab. Bei einem Einsatz des Sicherungsmoduls zur Herstellung fälschungssicherer Postwertzeichen ist die zur Überprüfung der Dokumente berechtigte Stelle der Postdienstbetreiber, beispielsweise die Deutsche Post AG. In diesem Fall hat eine Korrumperung eines Schlüssels eines Kundensystemanbieters eine sofortige postseitige Ablehnung jeglicher Transaktionen mit Sicherungsmodulen der Kundensystemhersteller zur Folge, deren signierte Lizenzen mit diesem Schlüssel hergestellt wurden.

Die Verwaltung der Schlüssel der Zertifizierungsstelle erfolgt entsprechend massgeblicher gesetzlicher und verwaltungsrechtlicher Bestimmungen. In Deutschland sind dies das Signaturgesetz SigG und die Signaturverordnung SigV. Eine weitere Erhöhung der Sicherheit durch Einbeziehung interner Bearbeitungsvorschriften ist möglich.

Die Schlüssel der Bescheinigungsstelle können jederzeit gewechselt werden, ohne dass hierbei Änderungen in den Kundensystemen erforderlich werden.

Nachfolgend wird ein Bescheinigungsverfahren anhand eines Einsatzes von symmetrischen Schlüsseln der Bescheinigungsstelle erläutert.

Symmetrische Schlüssel erlauben eine sehr schnelle Ver- und Entschlüsselung. Ein Einsatz von symmetrischen Schlüsseln setzt voraus, dass der Schlüssel des Senders und der Schlüssel des Empfängers übereinstimmen. Bei einer Kommunikation zwischen der Bescheinigungsstelle und einer Vielzahl von Kundensystemen können symmetrische Schlüssel dann eingesetzt werden, wenn die Bescheinigungsstelle über ausreichende Speicherkapazität für die einzelnen Schlüssel verfügt, die zu den jeweiligen Kundensystemen passen.

Ein Einsatz von asymmetrischen Schlüsseln sieht hingegen vor, dass der Sender die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und dass der Empfänger die Nachricht mit seinem privaten Schlüssel entschlüsselt.

Je nach Einsatzgebiet ist ein Einsatz von symmetrischen oder von asymmetrischen Schlüsseln vorzusehen. Die dargestellten Verfahren können jedoch grundsätzlich sowohl mit symmetrischen als auch mit asymmetrischen Schlüsseln erfolgen.

55 Sicherheitsrelevante Aufgaben des Sicherungsmoduls

Das Sicherungsmodul muss zur Initialisierung, zur Kommunikation mit der Bescheinigungsstelle und zur Deaktivierung im Wesentlichen folgende Aufgaben erfüllen:

60 Schlüsselerzeugung

Erzeugung und Speicherung eines asymmetrischen Schlüsselpaars innerhalb des Sicherungsmoduls.

65 Ausgabe des öffentlichen Schlüssels

Ausgabe des erzeugten öffentlichen Schlüssels im Rahmen der digitalen Signatur der Lizenz durch den Kundensystemhersteller.

stemanbieter (Issuer). Der private Schlüssel darf das Sicherungsmodul niemals verlassen.

Zertifikatspeicherung

Dauerhafte Speicherung des eigenen öffentlichen Schlüssels, beziehungsweise der eigenen signierten Lizenz im Rahmen der Initialisierung.

Signaturerzeugung

Erzeugung einer digitalen Signatur unter Verwendung des eigenen privaten Signaturschlüssels.

Signaturprüfung

Prüfung der digitalen Signatur eines Bescheinigungsmoduls der Bescheinigungsstelle unter Verwendung der signierten Lizenz der Bescheinigungsstelle und deren Zertifikat nach einer geeigneten Sicherheitsnorm, beispielsweise dem SigG.

Zertifikatprüfung

Prüfung eines Zertifikats durch Anfrage bei der Zertifizierungsstelle.

Temporäre Zertifikatspeicherung

Temporäre Speicherung eines Zertifikats oder einer signierten Lizenz im Rahmen einer Kommunikationssitzung.

Asymmetrische Verschlüsselung

Verschlüsselung von Daten mit einem verifizierten öffentlichen Schlüssel eines Kommunikationspartners.

Asymmetrische Entschlüsselung

Entschlüsselung von Daten mit dem eigenen privaten Schlüssel, die mit dem eigenen öffentlichen Schlüssel verschlüsselt wurden.

Zufallszahlerzeugung

Erzeugung und dauerhafte Speicherung einer nachweisbar qualitativ hochwertigen Zufallszahl in einem Zahlenraum von mindestens 16 byte.

Speicherung eines Sitzungsschlüssels

Temporäre Speicherung eines Sitzungsschlüssels mit einer Länge von 16 byte.

Speicherung von zwei Identifikationsnummern des Ladevorganges

Speicherung der jeweils zwei neuesten Identifikationsnummern mit einer Länge von jeweils 16 byte.

Speicherung des aktuellen Registerwerts der Wertbörse

Speicherung der Währung und des Betrags, der aktuell zur Herstellung von Freimachungsvermerken verwendet werden kann; "Descending Register".

Speicherung des aufsteigenden Registerwerts

Speicherung aller insgesamt mit dem Sicherungsmodul freigemachten Beträge, vorzugsweise in einer einheitlichen Währung, beispielsweise dem Euro; "Ascending Register".

Benutzeridentifikation

10 Persönliche Identifikation des für bestimmte Nutzungsmöglichkeiten berechtigten Benutzers des Sicherungsmoduls durch Verwendung einer mit dem eigenen öffentlichen Schlüssel zu verschlüsselnden PIN.

15 Statusausgabe der Identifikationsnummer des Ladevorganges

20 Ausgabe der Gültigkeit des aktuellen Ladesystems an das Kundensystem ohne die Möglichkeit der Änderung durch das Kundensystem.

Statusausgabe des Registerwerts der Wertbörse

25 Ausgabe des aktuellen verfügbaren Börsenwerts an das Kundensystem ohne die Möglichkeit der Änderung durch das Basissystem.

Hash-Bildung der sendungsspezifischen Daten

30 Bildung eines Hash-Wertes, beispielsweise nach SHA-1 von den vom Kundensystem übermittelten sendungsspezifischen Daten und der gespeicherten Zufallszahl.

Verminderung von Registerwerten einer Wertbörse

35 Vorzugsweise arbeitet das Sicherungsmodul mit einer digitalen Wertbörse zusammen. Diese Wertbörse kann in das Sicherungsmodul integriert sein oder separat untergebracht werden. Eine separate Unterbringung erfolgt beispielsweise in einer digitalen Brieftasche (Digital-Wallet). Durch die Speicherung wird sichergestellt, dass nur tatsächlich vorhandene Beträge benutzt werden. Bei der Benutzung, bei der beispielsweise eine Hash-Wert-Bildung erfolgt, wird der Betrag und damit auch der ihm zugeordnete Registerwert verringert.

Digitale Signatur der sendungsspezifischen Daten

40 Bildung und Ausgabe der Digitalen Signatur der sendungsspezifischen Daten bei jeder Hash-Bildung der sendungsspezifischen Daten.

Fehlerprotokollierung

45 Protokollierung der Aktivität sowie gültiger und ungültiger Kommunikationsversuche mit dem Sicherungsmodul.

Selbsttest

50 Durchführung eines Selbsttests bei jeder Aktivierung.

Deaktivierung

55 Deaktivierung des Sicherungsmoduls nach Identifikation und Aufforderung durch einen Operator.

60 Sicherheitsniveau durch Security Level nach FIPS PUB 140

65 Ziel des Sicherungsmoduls ist es, innerhalb eines Kun-

densystems die Vertraulichkeit und Integrität von Informationen, die im Sicherungsmodul gespeichert und verarbeitet werden, zu gewährleisten. Zur Erlangung eines einheitlichen Sicherheitsniveaus bei unterschiedlichen Kundensystemen und unterschiedlichen Sicherungsmodulen ist die Übereinstimmung mit und Zertifizierung nach einer vorher festgelegten Sicherheitsstufe, beispielsweise entsprechend einer durch FIPS PUB 140 vorgegebenen Sicherheitsstufe (FIPS PUB 140: "Security Level"), zweckmäßig.

Die Anwendung von FIPS PUB 140, Security Level 4, ist besonders vorteilhaft.

Die zur Durchführung empfohlene Sicherheitsstufe ist FIPS PUB 140, Security Level 3, weil hierdurch eine hohe Datensicherheit mit einem geringen Handhabungsaufwand verbunden werden.

Es ist besonders zweckmäßig, dass das System über FIPS PUB 140-1 hinausgehende Anforderungen erfüllt.

Zu einer weiteren Erhöhung der Datensicherheit ist es zweckmäßig, die sicherheitsrelevanten Prozesse des Kundensystems wie folgt durchzuführen:
Die Herstellung und Initialisierung des Sicherungsmoduls erfolgt in einer abgeschirmten Umgebung nach einem mit der Deutschen Post abgestimmten Sicherheitsstandard. Das Risiko der Korrumperung des zum Einsatz kommenden Signaturschlüssels zur Erzeugung der signierten Lizenzen der hergestellten Sicherheitsmodule wird durch Überprüfungen minimiert. Bei der Herstellung werden ein Schlüsselpaar erzeugt, ein öffentlicher Schlüssel zur Erzeugung der signierten Lizenz durch den Kundensystemanbieter ausgegeben, eine signierte Lizenz des Sicherungsmoduls (inklusive Sicherheitsmodul-ID) im Sicherungsmodul gespeichert und der Attributeintrag in einem eingesetzten Zertifikat gespeichert.

Aktivierung des Sicherungsmoduls durch das Kundensystem

Um vom Kundensystem aus das Sicherungsmodul zu aktivieren, wird dieses aufgefordert, seine signierte Lizenz (inklusive seines öffentlichen Schlüssels P_{SB}) sowie eine Zufallszahl X_{auth} mit einer Länge von 16 byte an das Kundensystem zu übergeben. (Die Zufallszahl dient insbesondere dann zur Absicherung von Replay-Attacken, wenn zwischen Tastatur des Kundensystems und Sicherungsmodul ein ungesicherter Übertragungswert liegt, etwa bei Internet Lösungen mit zentralem Sicherungsmodul-Server im Internet und dezentralen PCs als Eingabeterminals für Login-Informationen wie zum Beispiel PIN).

Fehlerbehandlung

Werden signierte Lizenz und Zufallszahl mehrmals, beispielsweise dreimal hintereinander angefordert, ohne dass anschließend Login-Daten vom Kundensystem an das Sicherungsmodul übertragen werden, muss dies im Sicherungsmodul protokolliert werden. Bei diesem Status darf ausschließlich eine anschließende Verbindung mit der Bescheinigungsstelle zur Fehlerbehebung mit Übertragung des Protokollstatus, nicht jedoch die Herstellung von fälschungssicheren Dokumenten wie Eintrittskarten oder Freimachungsvermerken, möglich sein.

Nach der Authentisierung des Kundensystems/Kunden liest das Sicherungsmodul die aktuelle Identifikationsnummer des Ladevorganges, die vorhergehende Identifikationsnummer, den aktuellen Wertbetrag und die Gültigkeit des Wertes und übergibt sie an das Basissystem. Eine Veränderung dieser Werte darf durch diesen Benutzer (FIPS PUB 140: role) in dieser Nutzungsmöglichkeit Benutzer

(FIPS PUB 140: service) nicht bestehen.

Patentansprüche

1. Sicherungsmodul, dadurch gekennzeichnet, dass es einen Dateneingang enthält, durch den Informationen in das Sicherungsmodul eingegeben werden können, dass das Sicherungsmodul wenigstens zwei Datenausgänge enthält, wobei durch einen ersten Datenausgang Daten ausgegeben werden können, die an eine Bescheinigungsstelle übertragen werden und wobei durch den zweiten Datenausgang Daten ausgegeben werden, die auf ein auszugebendes Dokument übertragen werden können, mit wenigstens zwei Kombinationsmaschinen (K1, K2), wobei eine erste der Kombinationsmaschinen (K1) einen Ergebniswert für den ersten Datenausgang erzeugt und wobei eine zweite Kombinationsmaschine (K2) einen Ergebniswert für den zweiten Datenausgang erzeugt.
2. Sicherungsmodul nach Anspruch 1, dadurch gekennzeichnet, dass es einen Geheimnisgenerator enthält, der ein nicht vorhersehbares Geheimnis erzeugt.
3. Sicherungsmodul nach Anspruch 2, dadurch gekennzeichnet, dass der Geheimnisgenerator mit der ersten Kombinationsmaschine und/oder der zweiten Kombinationsmaschine so verbunden ist, dass ein von dem Geheimnisgenerator erzeugtes Geheimnis in die erste Kombinationsmaschine (K1) und/oder die zweite Kombinationsmaschine (K2) eingeht.
4. Sicherungsmodul nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass es ein Identifikationsregister enthält, wobei ein Ausgangswert des Identifikationsregisters so mit der ersten Kombinationsmaschine (K1) verbunden ist, dass in eine von der ersten Kombinationsmaschine ausgegebene Datenkombination ein Wert des Identifikationsregisters eingeht.
5. Sicherungsmodul nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass es wenigstens eine Verschlüsselungsmaschine enthält, welche einen Ausgangswert einer der Kombinationsmaschinen (K1) verschlüsselt.
6. Sicherungsmodul nach Anspruch 5, dadurch gekennzeichnet, dass die Verschlüsselungsmaschine mit einem Schlüsselregister verbunden ist, wobei wenigstens ein in dem Schlüsselregister enthaltener Wert in der Verschlüsselungsmaschine zur Verschlüsselung eingesetzt werden kann.
7. Sicherungsmodul nach einem oder mehreren der vorangegangenen Ansprüche, dadurch gekennzeichnet, dass es eine Hash-Maschine enthält.
8. Verfahren zur Erstellung fälschungssicherer Dokumente, wobei Eingangsdaten in einen Dateneingang eines Sicherungsmoduls eingegeben werden und wobei in dem Sicherungsmodul zur Identifizierung einzelner Dokumente dienende Informationen erzeugt werden, dadurch gekennzeichnet, dass die Eingangsdaten in einen Dateneingang eines Sicherungsmoduls eingegeben werden, dort mit ein Geheimnis repräsentierenden Daten kombiniert werden und dass das Geheimnis in einem von dem Kombinieren getrennten Verarbeitungsschritt weiter verarbeitet wird und dass Daten aus der Kombination der das Geheimnis repräsentierenden Daten und der Eingangsdaten gewonnen werden.
9. Verfahren nach Anspruch 8, dadurch gekennzeichnet, dass das Geheimnis durch einen ersten Datenausgang ausgegeben wird und dass die Daten, die aus der Kombination der das Geheimnis repräsentierenden Da-

ten und der Eingangsdaten gewonnen werden, an einem zweiten Datenausgang ausgegeben werden.

10. Verfahren nach einem oder mehreren der Ansprüche 8 oder 9, dadurch gekennzeichnet, dass die Kombination der das Geheimnis repräsentierenden Daten und der Eingangsdaten in einer zweiten Kombinationsmaschine (K2) erfolgt.

11. Verfahren nach Anspruch 10, dadurch gekennzeichnet, dass die das Geheimnis repräsentierenden Daten und die Eingangsdaten irreversibel miteinander verknüpft werden, wobei die irreversible Verknüpfung so erfolgt, dass ausschließlich bei wiederholter Verknüpfung derselben Daten in derselben Weise ein identisches Ergebnis entsteht ohne dass Rückschlüsse auf das temporäre Geheimnis möglich sind.

12. Verfahren nach einem oder mehreren der Ansprüche 8 bis 11, dadurch gekennzeichnet, dass die weitere Verknüpfung der das Geheimnis repräsentierenden Daten unter Einbeziehung von Daten eines Identifikationsregisters erfolgt.

13. Verfahren nach Anspruch 12, dadurch gekennzeichnet, dass das Ergebnis der Kombination der Daten, die das Geheimnis repräsentieren und der Daten des Identifikationsregisters (ID) in einer Verschlüsselungsmaschine verschlüsselt wird.

14. Verfahren nach Anspruch 13, dadurch gekennzeichnet, dass die Verschlüsselung unter Einbeziehung eines Schlüssels erfolgt, dessen Wert in einem Schlüsselregister (SR) gespeichert ist.

15. Verfahren nach einem oder mehreren der Ansprüche 8 bis 14, dadurch gekennzeichnet, dass die Daten, die aus dem ersten Datenausgang ausgegeben werden, an eine Bescheinigungsstelle übertragen werden.

16. Verfahren nach Anspruch 15, dadurch gekennzeichnet, dass die Bescheinigungsstelle die Daten mit einem weiteren Schlüssel verknüpft.

17. Verfahren nach einem oder mehreren der Ansprüche 8 bis 16, dadurch gekennzeichnet, dass die Daten, die aus dem zweiten Datenausgang ausgegeben werden als fälschungssichere Informationen auf die zu erstellenden fälschungssicheren Dokumente ausgegeben werden.

Hierzu 1 Seite(n) Zeichnungen

45

50

55

60

65

- Leerseite -

